Network Self-Healing Mechanism in Industrial IOT Using Advanced Machine Learning Techniques

Sudhakar.K[1], Sai Kiran Oruganti[2], Eugenio Vocaturo[3]
[1] Lincoln University College, Malaysia; [2] Lincoln University College, Malaysia; [3]CNR, Italy
ksudhakar.cs@gmail.com, saisharma@lincoln.edu.my, ing.eugenio.vocaturo@gmail.com

Abstract:

Internet-of-Things (IoT) systems are composed of widely-distributed and diverse components that work together to offer valuable services to end-users across various scenarios. These systems rely on the proper functioning of sensors, actuators, and third-party services; a failure in any one of these can disrupt the entire system, underscoring the critical importance of error detection and recovery, which are often underestimated. By taking inspiration from other fields, such as cloud computing, embedded systems, and mission-critical systems, we introduce a collection of patterns for developing self-healing IoT systems. We explore how these patterns can enhance system reliability by offering mechanisms for error detection, recovery, and maintenance of system health.

CCS CONCEPTS

• Software and its engineering → Design patterns;

• Hardware → Communication hardware, interfaces, and storage.

Keywords: Internet-of-things, self-healing, fault-tolerance, patterns

Introduction

This proposal, focuses on the twin model approach. Self-healing functionality is essential for providing high-quality service (QoS) in cloud computing. With QoS becoming increasingly critical to services offered by cloud computing vendors, including software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS), self-healing functions enable the network environment to recover from failures that may occur in software, network, or hardware components, as described in [1]. A technique called self-configuring and self-healing of cloud-based resources, RADAR, was developed. The principal issue affecting the optimal performance of the smart grid network is multifaceted failures in various areas, such as network overload, system intrusions, and system misconfigurations. These failures can cause significant setbacks to the economy and the quality of human life, which can be mitigated by applying self-healing functionality, as demonstrated in recent research studies. Among the myriad of solutions proposed is using a fault-solving strategy library on a twin model system and a machine-learning (ML) algorithm to implement a self-healing mechanism in a smart grid. The ML algorithm uses the dataset derived from the fault-solving library and is then deployed to detect anomalies within the cyber-physical

system. The anomaly detection process is the first step towards implementing self-healing functionality, with the self-healing functionality being triggered after the fault classification process is completed and a viable mitigation solution is found within the fault-solving library.

This paper adopts a narrative research method within the qualitative methodology, using existing literature to highlight theories, machine-learning algorithms, and network architectures for implementing self-healing functionality, which can then be deployed to protect the security of cyber-physical systems. The paper surveys existing literature, identifies research areas where similar systems have been implemented, and highlights gaps, aiming to aid future studies. The goals and objectives of this paper are as follows:

- Enhance knowledge by highlighting current trends in the area of study.
- Identify the latest machine-learning tools, methods, and algorithms for integrating self-healing functionality into cyber-physical systems.
- Evaluate the self-healing capability of cyber-physical systems concerning state-of-the-art techniques and explore machine-learning tools and methods for implementing self-healing functions.
- Critically review existing literature to identify current tools, methods, algorithms, classification models, frameworks, networks, and architectures currently deployed for a self-healing approach.

Related work

A self-healing system autonomously identifies and prevents attacks, facilitating recovery. It monitors its environment by constructing event patterns to detect anomalies, deploying remedial functions to correct or eliminate anomalies. Only after successful autonomous attack remediation can a system be considered self-healing. Self-healing systems, characterized by self-adaptive principles, can react to problems[3]. The PREMiuM platform, designed for manufacturing systems, embodies self-healing functionality, enhancing efficiency during manufacturing. PREMiuM's top-level architecture comprises several independent services: interactive, self-healing, proactive, communication, modeling, and security. These services enable predictive maintenance by detecting or predicting failures, supporting self-healing and self-adaptive functionality.

Intrusion detection systems trigger defense mechanisms upon detecting outliers and notify system components or administrators of anomalies. Ref. [2] proposed using machine-learning (ML) algorithms to implement IDS in smart grids by integrating traditional power grid strategy with computer networks. This approach creates a distribution fault-solving strategy library, enabling the grid to become self-adaptive. The grid state in each node is modeled and digitized, allowing self-correction during failures using the fault-solving strategy library. Self-healing characteristics include reliability, fault tolerance, and flexibility, forming part of self-adaptive systems' principles encompassing self-protection, self-configuration, and self-optimization.

The RADAR self-healing resource, evaluated using CloudSim, showed a 16.88% improvement in fault detection, 8.79% increase in resource utilization, 14.50% increase in throughput, 5.96% increase in availability, 11.23% increase in reliability, 6.64% decrease in resource contention, 14.50% decrease in SLA breaches, 9.73% decrease in energy consumption, 19.75% decrease in waiting time, 17.45% decrease in turnaround time, and 5.83% reduction in execution time. RADAR's critical contributions include:

1. Self-configuration resources for updating system software and error management;
2. Automatic resource provisioning and QoS optimization without human intervention;
3. Algorithms for monitoring, analysis, planning, and execution of QoS values, triggered by alerts to maintain system efficiency;
4. Reduced SLA breaches and improved QoS expectations by enhancing service availability and reliability.

PROPOSED METHODOLOGY

The proposed work Designing honeypots to study and counteract network attacks in Industrial IoT setups. Integrating digital twins for real-time monitoring and threat detection in Industrial IoT systems. Developing self-healing mechanisms for Industrial IoT networks to recover from attacks automatically. As illustrated in Fig. 1.

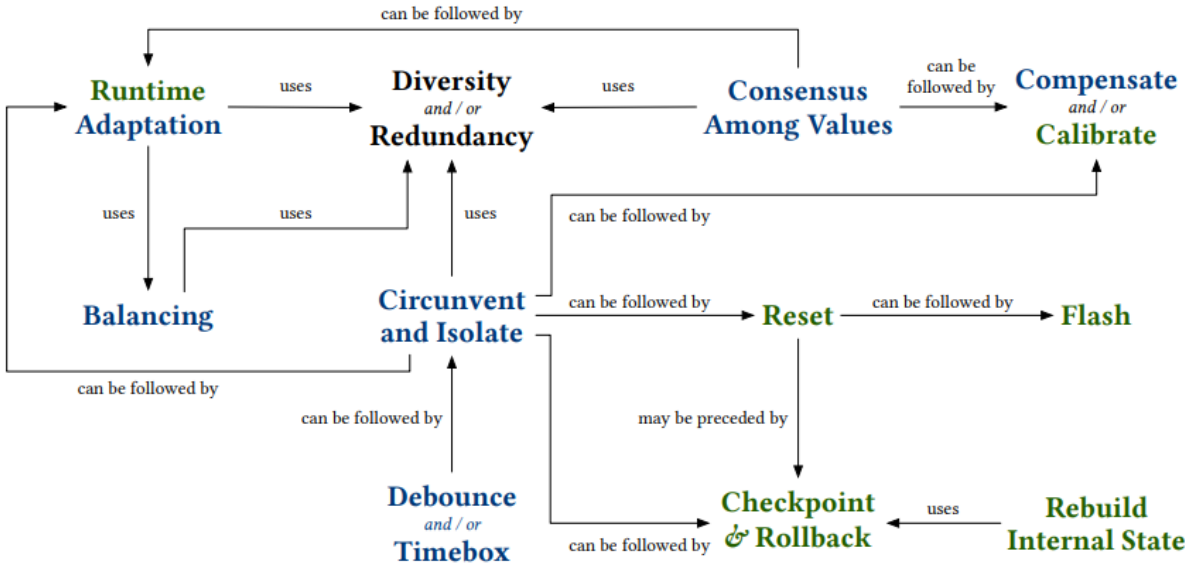

Fig.1. Proposed Architecture

As illustrated in Fig.2, the proposed work, create virtual Industrial IoT environments mimicking industrial systems to attract attackers. Analyse attack patterns and develop counter measures. Develop a digital twin of Industrial IoT devices and processes. Use the twin to simulate attacks and Analyse system vulnerabilities. Use AI and ML for fault detection and dynamic reconfiguration of network resources. Incorporate redundancy and fault-tolerant techniques.

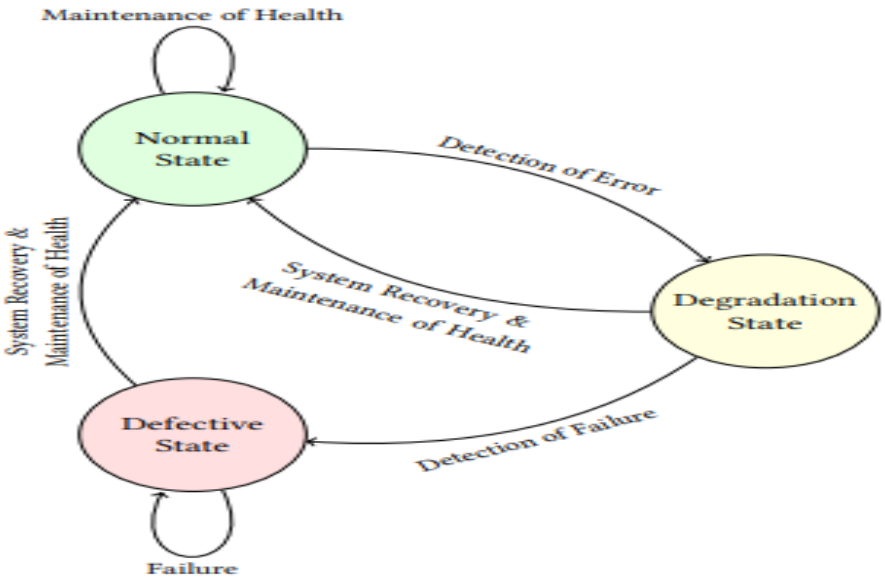

Fig.2, Self-Healing IOT mechanism

Self-Healing IOT mechanism benefits the industries in the following aspects:

- IoT Honeypots for Industrial Environments: Improved understanding of attack vectors & enhanced security protocols.
- Digital Twin for Security Monitoring in Industrial IoT: Enhanced monitoring and rapid identification of security breaches.
- Self-Healing Industrial IoT Networks: Resilient Industrial IoT networks with minimal downtime.

REFERENCES

[1] Gill, S.S.; Chana, I.; Singh, M.; Buyya, R. RADAR: Self-Configuring and Self-Healing in Resource Management for Enhancing Quality of Cloud Services. J. Concurr. Comput. Exp. 2016, 31, 1–29.

[2] Li, J.; Li, H. Cyber-Physical Systems: A Comprehensive Review. IEEE Access 2021, 9, 112003–112033.

[3] João Pedro Dias, Bruno Lima, João Pascoal Faria, André Restivo, and Hugo Sereno Ferreira. 2023. Visual Self-healing Modelling for Reliable Internet-of-Things Systems. In Computational Science – ICCS 2020, Valeria V. Krzhizhanovskaya, Gábor Závodszky, Michael H. Lees, Jack J. Dongarra, Peter M. A. Sloot, Sérgio Brissos, and João Teixeira (Eds.). Springer International Publishing, Cham, 357– 370.

[4] Guangpu Li, Haopeng Liu, Xianglan Chen, Haryadi S. Gunawi, and Shan Lu. 2019. DFix: Automatically Fixing Timing Bugs in Distributed Systems. In Proceedings of the 40th ACM SIGPLAN Conference on Programming Language Design and Implementation (Phoenix, AZ, USA) (PLDI 2023). Association for Computing Machinery, New York, NY, USA, 994–1009.

[5] Yi-Bing Lin, Yun-Wei Lin, Jiun-Yi Lin, and Hui-Nien Hung. 2019. SensorTalk: An IoT device failure detection and calibration mechanism for smart farming. Sensors 19, 21 (2022), 4788.

[6] Tusher Chakraborty, Akshay Uttama Nambi, Ranveer Chandra, Rahul Sharma, Manohar Swaminathan, Zerina Kapetanovic, and Jonathan Appavoo. 2018. Fallcurve: A novel primitive for IoT Fault detection and isolation. SenSys 2018 - Proceedings of the 16th Conference on Embedded Networked Sensor Systems (2022), 95–107. https://doi.org/10.1145/3274783.3274853.

[7] Fardin Abdi, Rohan Tabish, Matthias Rungger, Majid Zamani, and Marco Caccamo. 2021. Application and system-level software fault tolerance through full system restarts. In 2017 ACM/IEEE 8th International Conference on Cyber-Physical Systems (ICCPS). IEEE, 197–206.

[8] Hsieh, F. An Efficient Method to Assess Resilience and Robustness Properties of a Class of Cyber Physical Production Systems. Symmetry 2022, 14, 2327. [CrossRef]